Cybersecurity in the Time of COVID-19

03/23/2020

As the COVID-19 pandemic continues, hackers continue to target workers' increased dependence on digital tools. Online activities have become the most effective channel for human interaction and continued operations. In current circumstances, a cyberattack removing a household or business's ability to connect via their devices could be catastrophic. The US Department of Health and Human Services has already been targeted with an intent to disrupt the flow of information.[1]

Despite an ebbing flow of anxiety for many, it is important to "keep cool" regarding online activities as most of America continues or begins to work from home. Increased time spent online inadvertently increases risky behavior that may make a user more susceptible to attacks. Here are some practices that can be implemented to stay safe online and operationally:

Practice Good Cyber Hygiene Individually

- Ensure your home Wifi password meets the password standards implemented at your office
- Confirm system firewalls are active on your router
- Use virtual private network (VPN) for internet access if available
- Be aware of suspicious emails, downloads or USB drives that could introduce malicious software into your computer or network
- Ensure any new programs or apps installed are from a trusted source
- Install anti-virus software patches and updates to all devices on your home network
- Store data on available encrypted network drives to avoid loss
- Do not respond to email solicitations asking for personal or financial information
- Avoid clicking on links and attachments in unsolicited emails
- Be aware of hidden risks related to "free" access sites and applications
- Be mindful of surfing habits
- Remember your cybersecurity training

Maintain Legally-Compliant Business Practices

- Stick to your established procedures regarding personal information collection
- Do not forget the privacy laws that apply to your organization – although these are trying times, they still apply
- Keep the scope of personal information collected by your organization limit to what is necessary and appropriate
- Consider updating controls and safeguards of any new categories of personal information that is being collected
- Remind employees of the types of information that require safeguarding
- Restrict sharing work computers and devices with other members of an employee's household
- Implement multi-factor authentication
- Utilize encryption at rest and in transit where possible

- Review business continuity and remote work access policies
- Have a communication plan in place
- Proactively review insurance coverage in the event of a disruption
- Keep IT resources and staff well stocked and staffed

As people settle into a new normal, the work environment will inevitably slow down, leading to users engaging in less-than-best practices to be efficient. It is important to be patient, remember your cybersecurity training and be vigilant to identify things that are out of place or unusual. Doing so will reduce the likelihood of falling victim to malicious attacks, outages and errors.

---

[1] https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response?sref=BWbpWjRm